Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
NOV 2014	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
NDIA Hard Problems Workshop Cyber COl Deep Dive (U)	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **AFRL/RI, 525 Brooks Rd, Rome NY 13441-4505**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**41**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

The overall classification of this briefing is
UNCLASSIFIED

NDIA Hard Problems Workshop - Cyber COI Deep Dive

5 Nov 14

Dr. Richard Linderman

Cyber COI Steering Group Lead

Outline

- BLUF
- **Cyber COI Overview**
- Roadmap Development Process
- Cyber COI "4 + 2" S&T Roadmaps and Recent Successes
- Hard Problems and Gaps
- Engagements, Way Ahead, and Opportunities
- Summary

BLUF – Bottom Line Up Front

- Established, mature, and coordinated community
- Cyber S&T aligned to expanding operational capability gaps/priorities
- Cyber S&T contributions to nearly all Seven DoD Hard Problems
- Driving deeper engagement with industry and international partners

S&T Influencing the DoD Cyber Landscape

"...we will continue to invest in capabilities critical to future success, including... operating in anti-access environments; and prevailing in all domains, including cyber."

- President Obama, January 2012

Cyber Investment Management Board (CIMB)

COCOMs

Department of Defense Strategy for Operating in Cyberspace

CYBERSPACE POLICY REVIEW

TRUSTWORTHY CYBERSPACE: STRATEGIC PLAN FOR THE FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT PROGRAM

S&T Community of Interest

Enhance United States National Security & Economic Prosperity

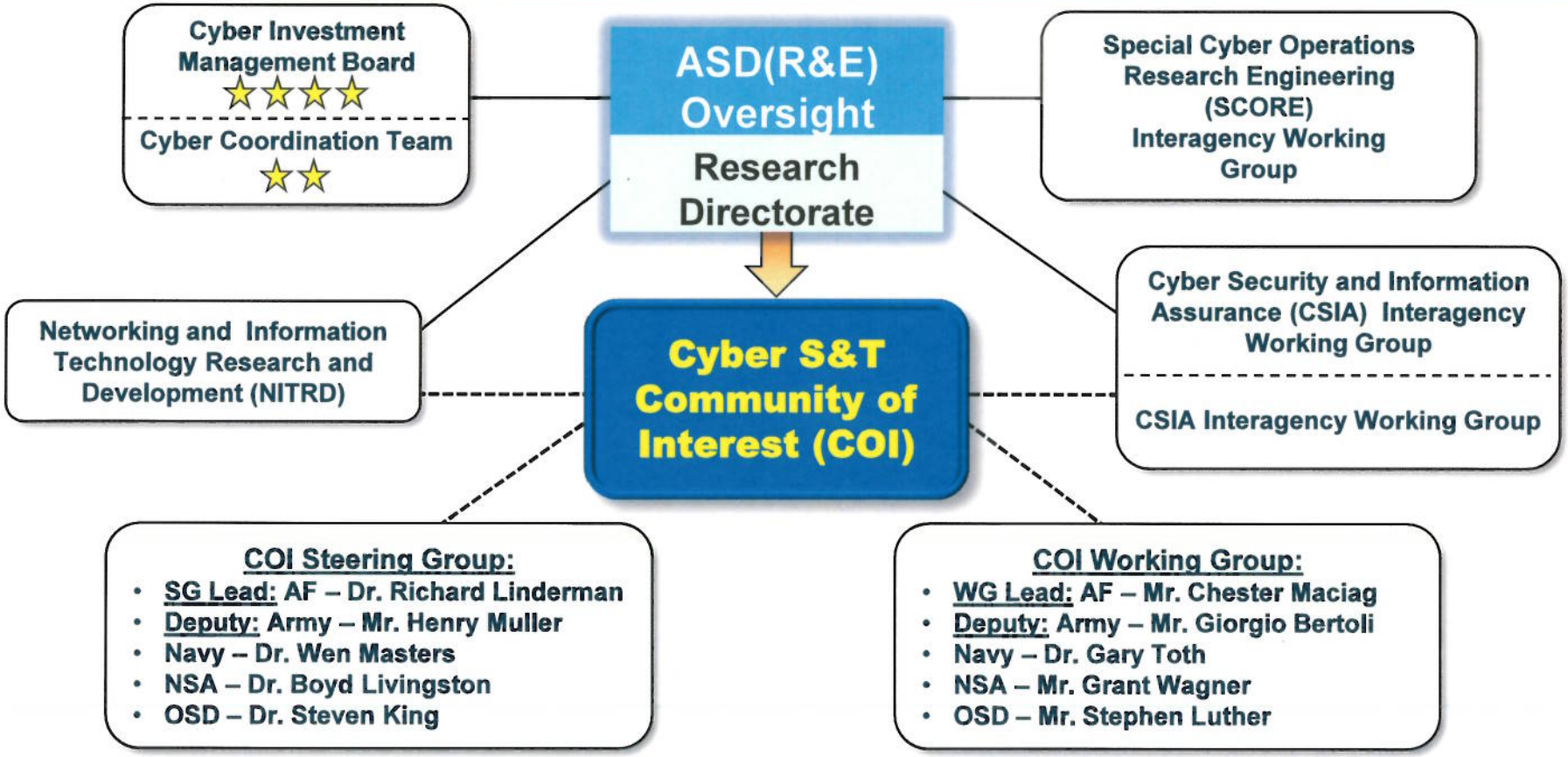
Defend the Homeland

Build Security Globally

Project Power and Win Decisively

Mission Assurance
Agility
Resiliency
Foundations of Trust

DoD Cyber S&T Coordination



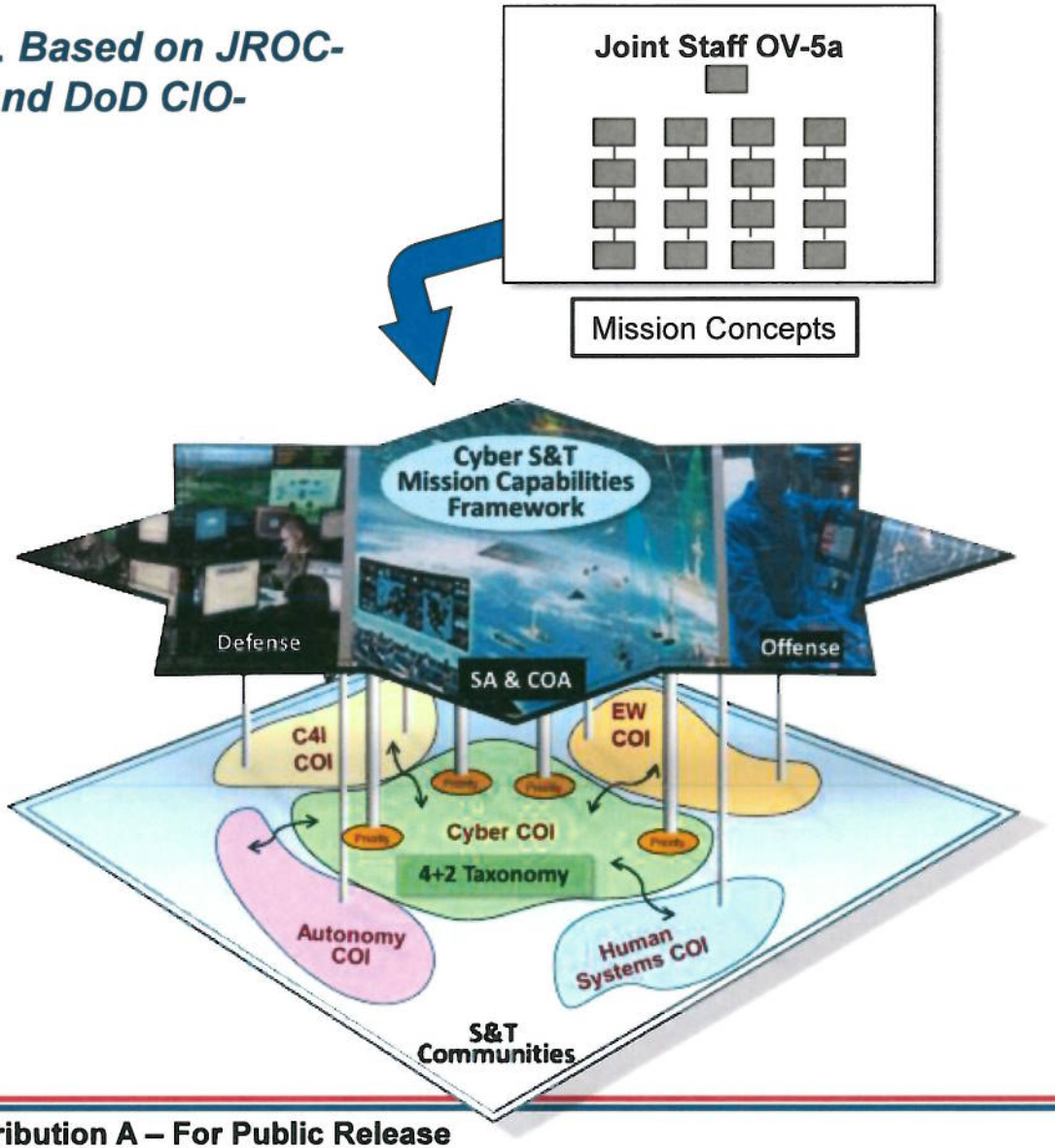
Users			Research Community						Users	
DISA	NSA IAD	DCIO	ONR/ NRL	AFRL/ AFOSR	NSA Research	DARPA	RDECOM	DTRA	USSTRATCOM/ USCYBERCOM	USD(I)

Community of Interest and Working Groups are the primary means for oversight, collaboration, & coordination

Cyber COI - Scope

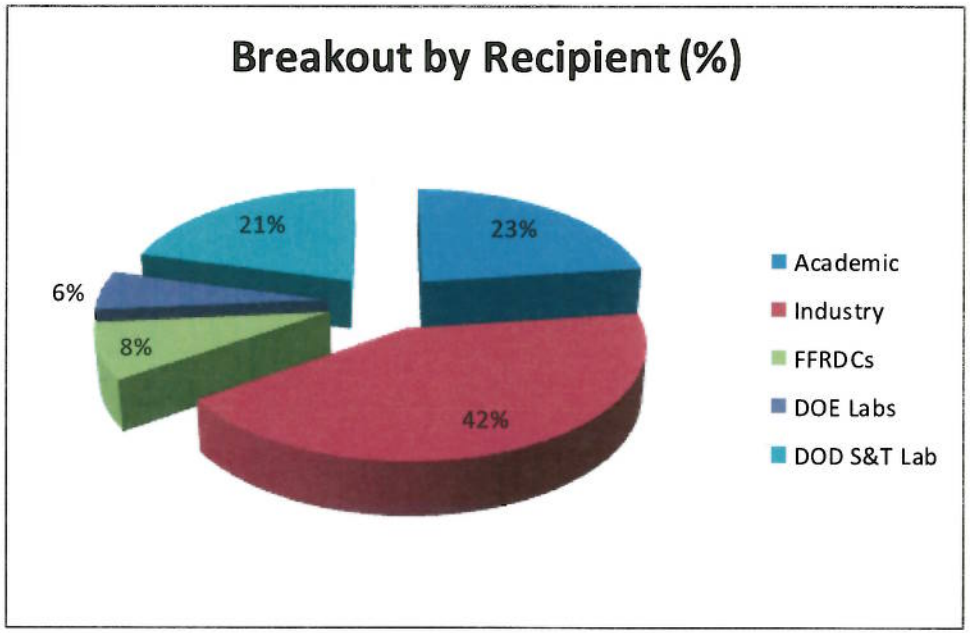
An Operational Domain: JS OV-5a. ***Based on JROC-Approved Capability Documents and DoD CIO-developed Architectures***

- Spans Defense, Effects, Situational Awareness-Course of Action
- Includes enterprise, tactical and embedded
- Cuts across all domains
- Touches C4I, EW, Autonomy, and Human Systems COIs
- Transcends S&T across all DOTMLPF
- QDR Tenets Addressed
  - Mitigates Threats
  - Delivers Affordable Capability
  - Affords Technological Surprise



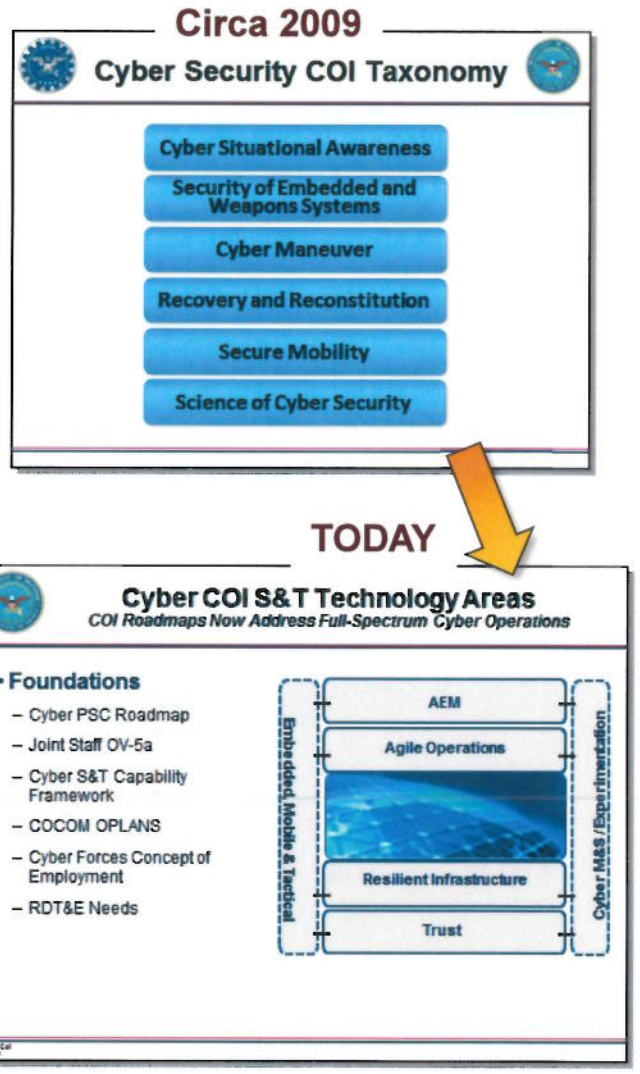
DoD Cyber S&T: Performers
(FY14 Execution)

- **Service S&T Labs**
  - AFRL, RDECOM, NRL, SPAWAR
- **DoD Agencies**
- **DoE Labs**
- **FFRDCs**
- **Industry**
- **Academia**



Cyber COI Recent Activities

- **(U) Briefed roadmap to S&T EXCOM in May**
  - (U) Cyber PSC → Cyber [Security] COI
  - (U) Incorporated findings of Cyber Investment Management Board
  - (U) High-level cyber S&T metrics
- **Evolving toward a Level 4 COI**
  - (U) International: Working multilateral cyber S&T agreements
  - (U) Academic: HBCU-MI Cyber Center of Excellence
  - (U) Industry: Engagement and collaboration leading to strategic Reliance



Outline

- BLUF
- Cyber COI Overview
- **Roadmap Development Process**
- Cyber COI "4 + 2" S&T Roadmaps and Recent Successes
- Hard Problems and Gaps
- Engagements, Way Ahead, and Opportunities
- Summary

Cyber S&T Roadmap Evolution

CIMB Driven Developments

Technology Challenges

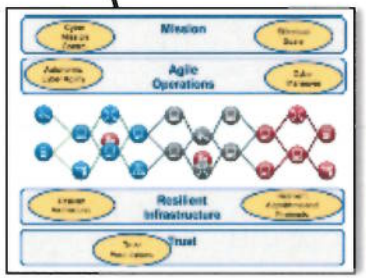
Cyber S&T Capability Framework

Way Ahead: CIMB & Cyber Metrics Maturation

2009 | 2010 | 2011 | 2012 | 2013 | 2014

COI | PSC | COI

GOF Study 4.18 DoD S&T Investment in Cyberspace Security and Information Assurance



Cyber Forces Concept of Employment

Roadmap Development and Priority Gaps

Cyber S&T Capability Framework

From CIMB Analysis of JS OV-5

Defense

- Reduce attack surface and increase resiliency of DODIN
- Reduce attack surface and increase resiliency of embedded/weapons systems
- Discover, understand, and engage threats

Engagement

- Active defense
- Respond to large-scale threats

Situational Awareness and Courses of Action

- Cyberspace situational awareness
- Understand cyber dependencies of missions
- Integrated course of action, cyber and non-cyber

Cyber S&T Capability Framework
Examples of High Level Metrics

Defense

- Increase total resources required by an adversary to achieve an effect
- Reduce adversary dwell time
- Reduce time until defense forces are aware of adversary

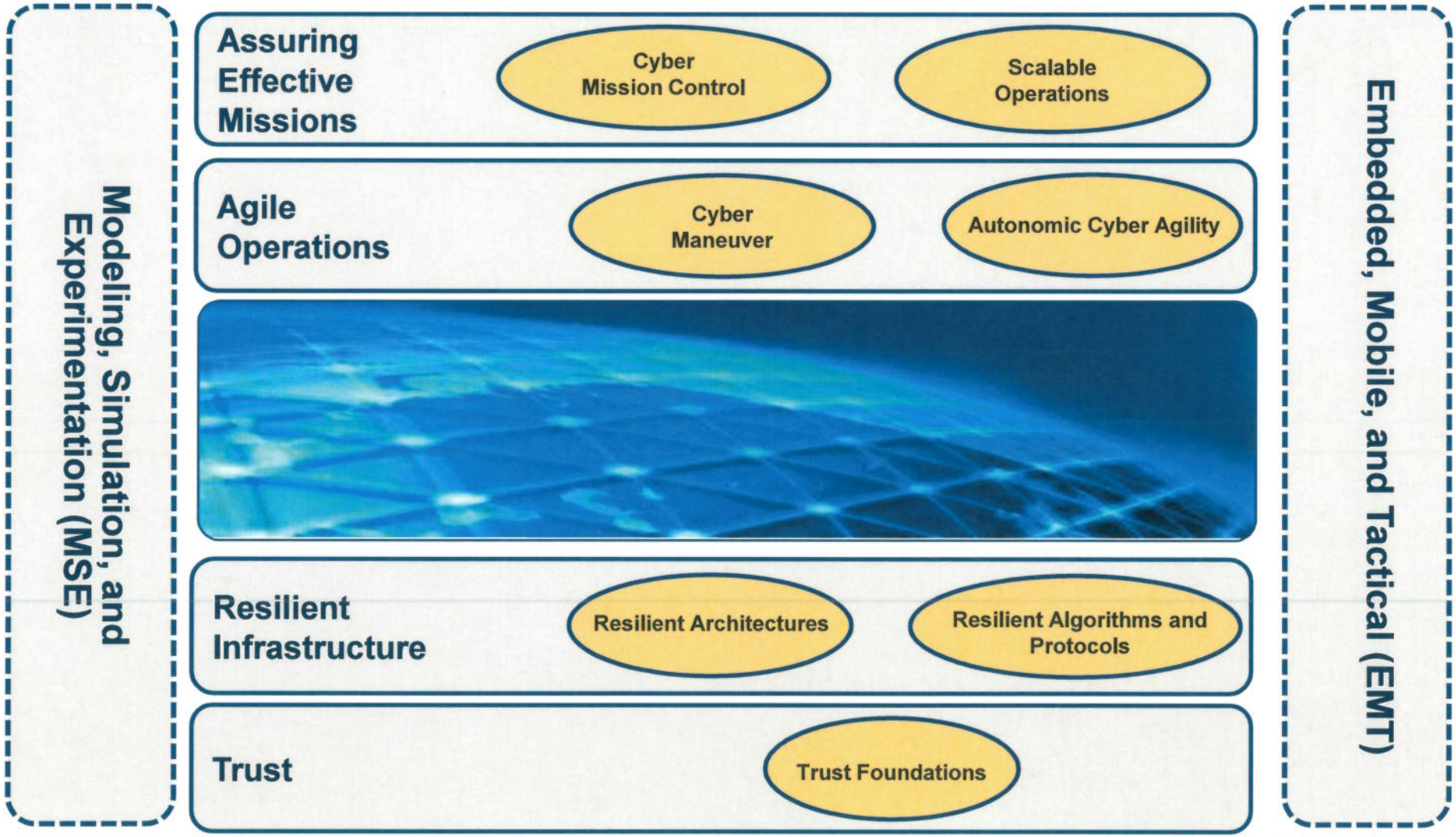
Engagement

- Increase cyber readiness
- Increase sophistication of campaign plans

Situational Awareness and Courses of Action

- Reduce time to map mission dependencies on cyber assets
- Improve robustness of mission-to-cyber mapping
- Increase quality of generated COA's

Cyber S&T Roadmap
Technology Challenges & Cross Cutting Areas



DoD's Joint Cyber S&T Focus Areas

Assuring Effective Missions	Assess & control the cyber situation in mission context
Agile Operations	Escape harm by dynamically reshaping cyber systems as conditions/goals change
Resilient Infrastructure	Withstand cyber attacks, while sustaining or recovering critical functions
Trust	Establish known degree of assurance that devices, networks, and cyber-dependent functions perform as expected, despite attack or error
Embedded, Mobile, & Tactical (EMT)	Increase the capability of cyber systems that rely on technologies beyond wired networking and standard computing platforms
Modeling, Simulation, & Experimentation (MSE)	Simulate the cyber environment in which the DoD operates to enable mission rehearsal and a more robust assessment and validation of cyber technology development

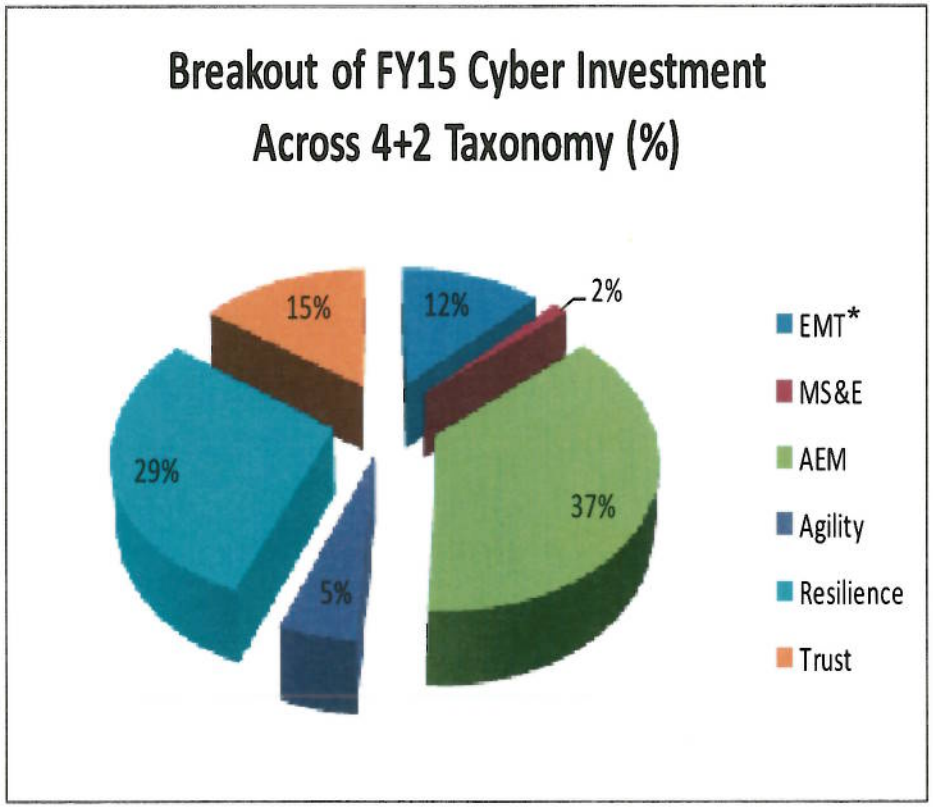
CROSS CUTTING

Outline

- BLUF
- Cyber COI Overview
- Roadmap Development Process
- **Cyber COI "4 + 2" S&T Roadmaps and Recent Successes**
- Hard Problems and Gaps
- Engagements, Way Ahead, and Opportunities
- Summary

Cyber FY15 S&T Across 4+2 Technology Areas

- **Funding Observations**
  - Appropriately increasing emphasis in AEM and EMT
  - Continued strong demand for Resilience
  - Trust focuses on military-unique topics
  - Agility operational goals and tradeoffs under discussion
  - Under-investment in MS&E resulting in acquisition and operational gaps

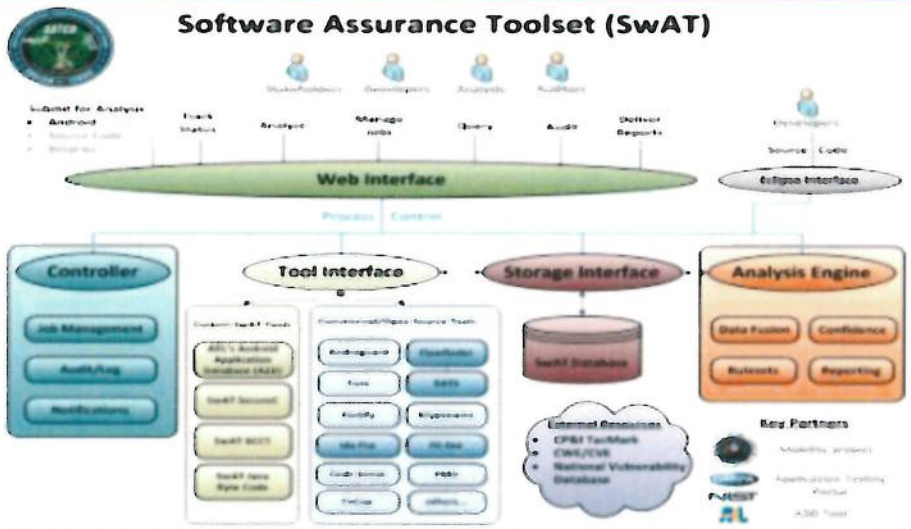


**Note: The EMT figures include some overlap with the other technology areas.*

Trust Foundations
Objectives / Accomplishments / Challenges

Objectives:

- **Trusted Components and Architectures**: Develop measures of trustworthiness for cyber components and large systems of varying pedigree and trustworthiness
- **Scalable Supply Chain Analysis and Reverse Engineering**: Analyze, attribute, and repurpose hardware and software at the speed and scale required for real-time strategic engagement



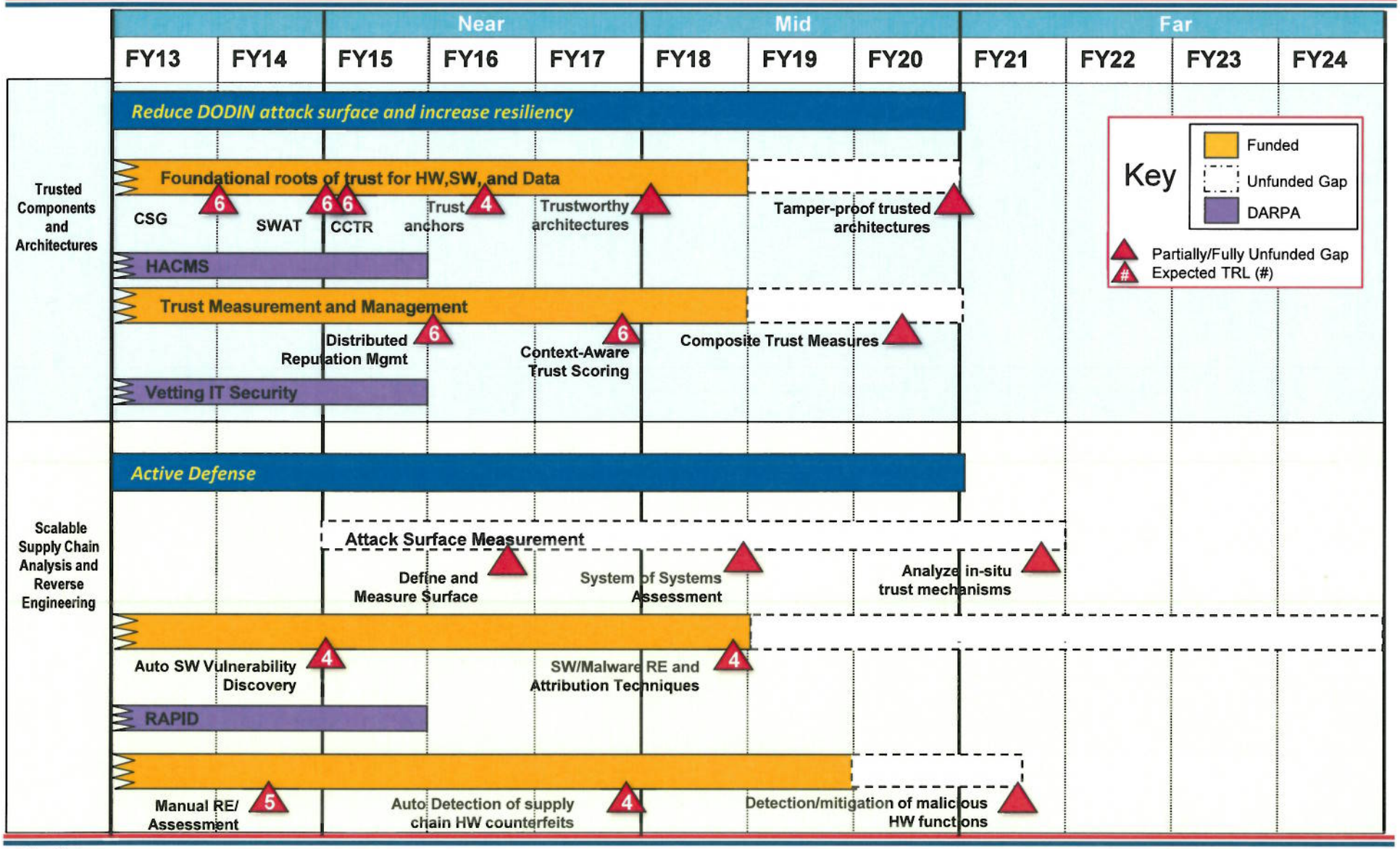
Accomplishments:

- FY13/14 Success Stories
  - Army: SW Assurance Toolkit (SWAT)
  - AF: Secure Processor
  - AF: Context/Content Aware Trusted Router
  - AF: Secure View

Technical Challenges:

- Development of Trust Anchors for component-level and composed HW and SW
- Tamper-proof/evident HW and SW components and systems
- Contextual threat/trust scoring calculus
- Rapid, assisted, and automated HW and SW analysis and validation
- Algorithms for accurate attribution of malware authors and supply chain tampering

Trust Foundations Roadmap

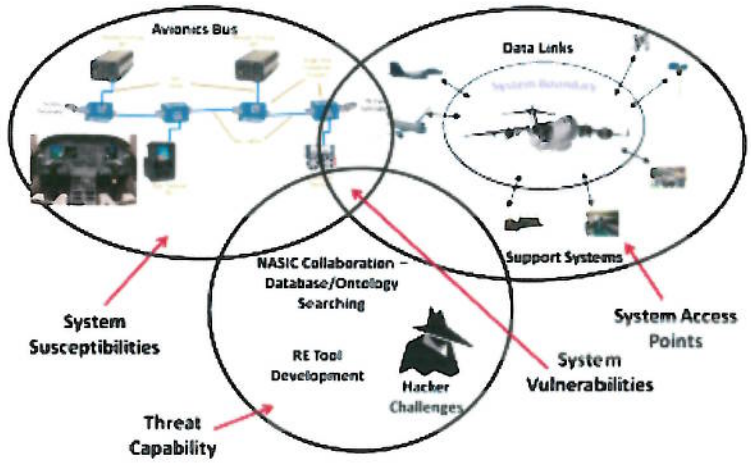


Resilient Infrastructure

Objectives / Accomplishments / Challenges

Objectives:

- **Resilient Architectures:** Develop integrated architectures that are optimized for the ability to absorb shock and speed recovery to a known secure operable state.
- **Resilient Algorithms and Protocols:** Develop novel protocols and algorithms to increase the repertoire of resiliency mechanisms available to the architecture that are orthogonal to cyber threats.



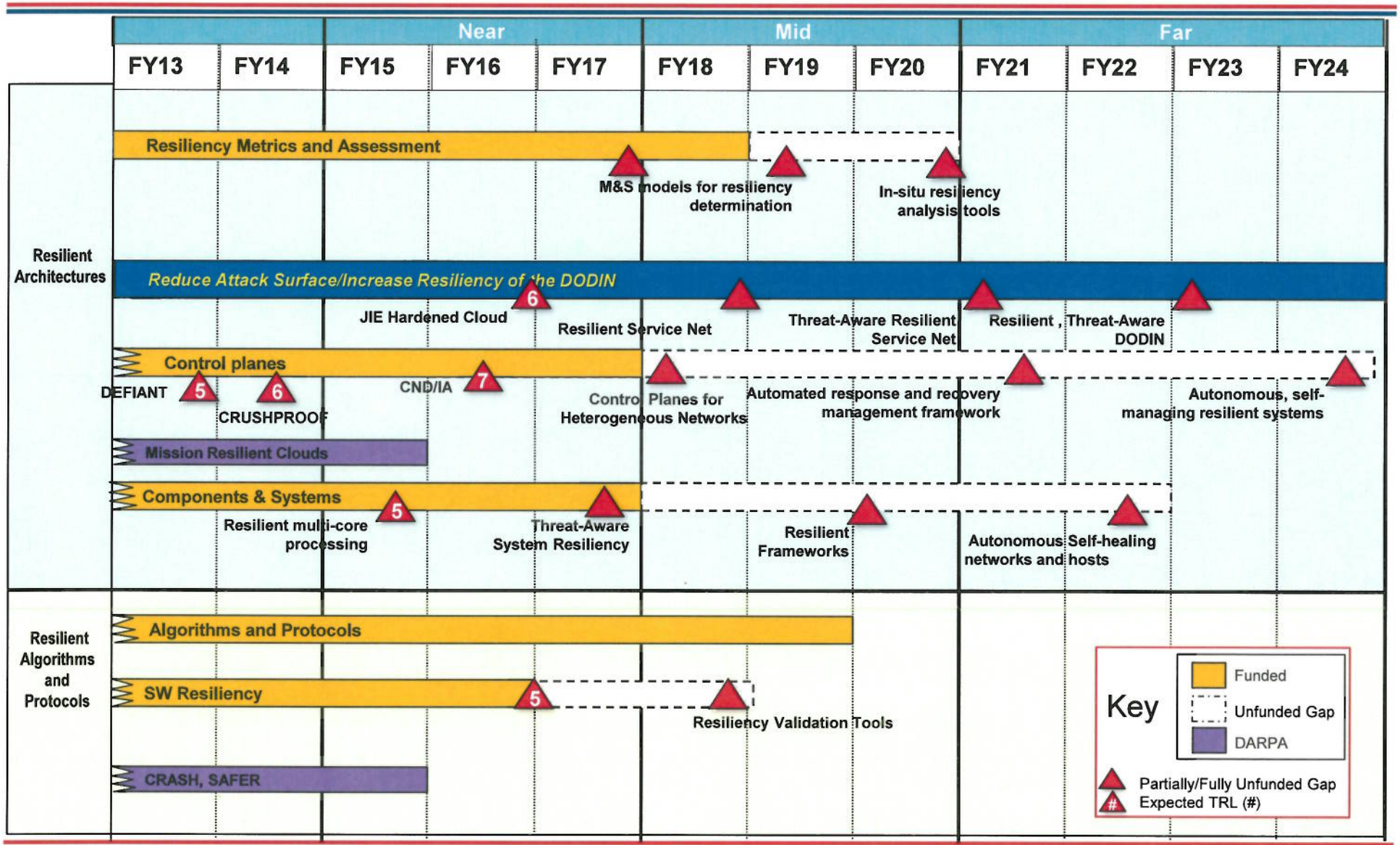
Accomplishments:

- FY13/14
  - Army DEFIANT
  - Army: CRUSHPROOF

Technical Challenges:

- Assessment environments and tools for measuring resiliency of HW, SW, networks, and systems
- Calculus for relating resiliency concepts into measurable operational impact and automated DODIN defense actions
- Resilient overlay control planes that orchestrate defense of heterogeneous DODIN systems
- Secure, LPI/J, energy-efficient, mobile communication protocols
- Certifiable, agile, and affordable mobile device HW, OS, and app ecosystem

Resilient Infrastructure Roadmap

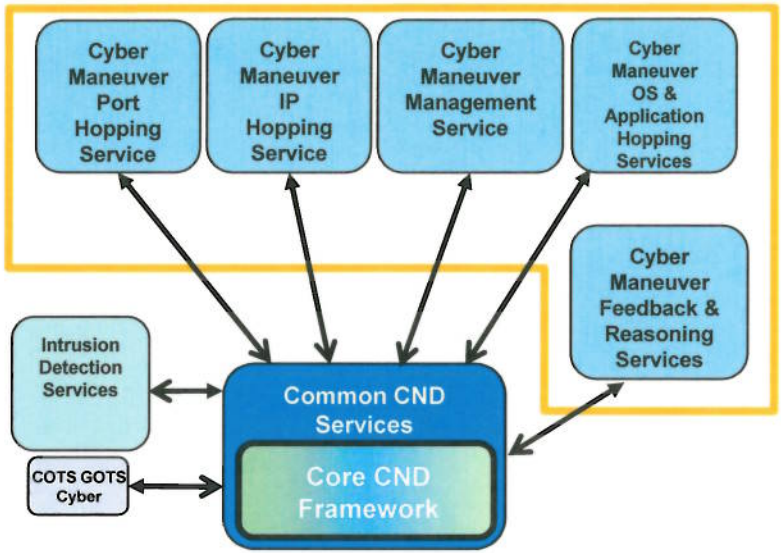


Agile Operations

Objectives / Accomplishments / Challenges

Objectives:

- **Cyber Maneuver:** Develop mechanisms that enable dynamically changing cyber assets to be marshaled and directed toward an objective – to create or maintain a defensive or offensive advantage
- **Autonomic Cyber Agility:** Speed the ability to reconfigure, heal, optimize, and protect cyber mechanisms via automated sensing and control processes



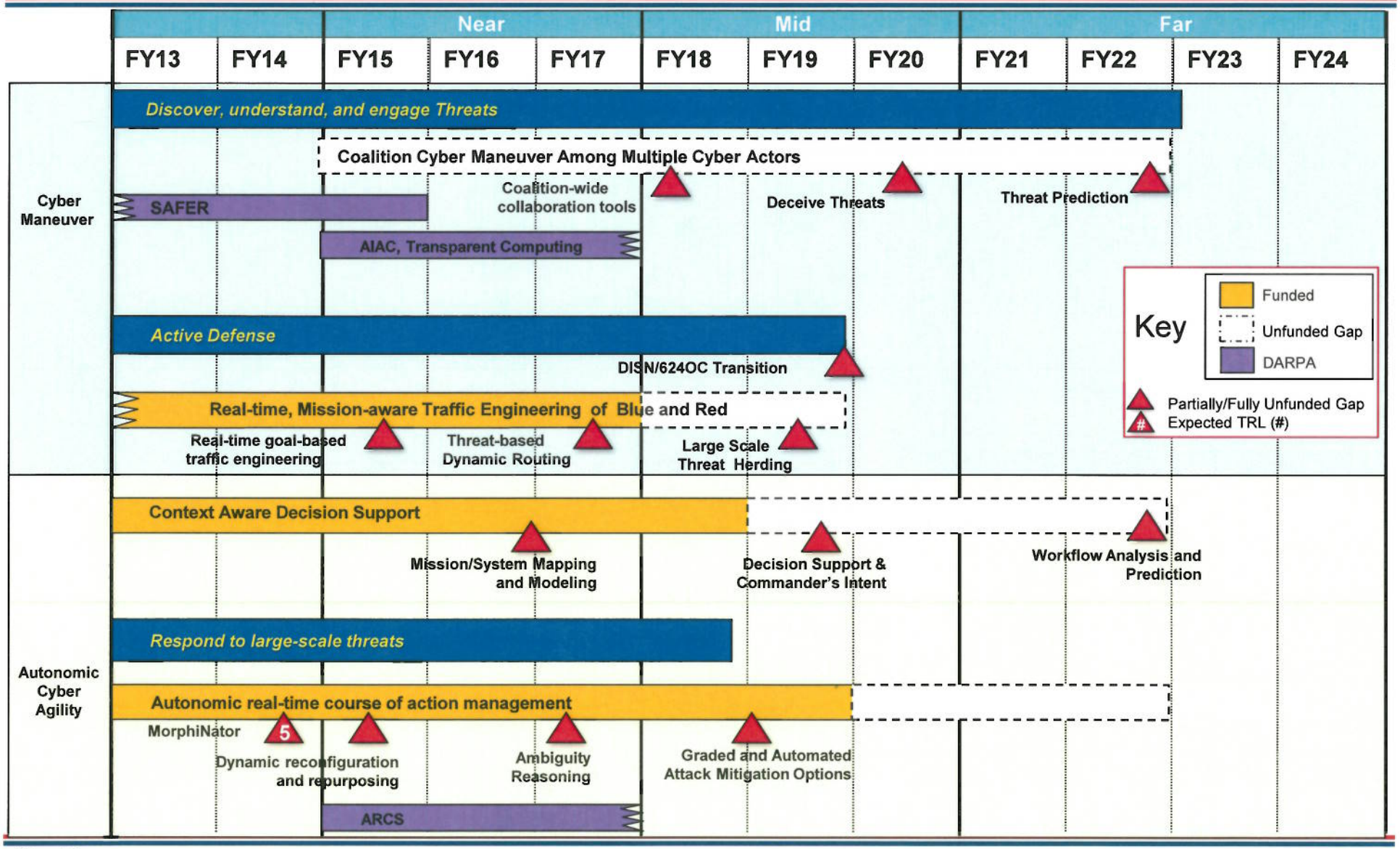
Accomplishments:

- Army: MorphiNator
- AF: ARCSYNE/COSYNE

Technical Challenges:

- Real-time, mission-aware traffic engineering including routing of threats
- Collaborative, coordinated cyber maneuver of multiple actors and forces (including coalition)
- Cyber maneuver for deceiving threats
- Dynamic reconfiguration of networks, systems and applications
- Autonomous reconfiguration

Agile Operations Roadmap



Assuring Effective Missions
Objectives / Accomplishments / Challenges

Objectives:

- **Cyber Mission Control:** Develop tools and techniques that enable efficient models of cyber operational behaviors (cyber and kinetic) to determine the correct course of action in the cyber domain
- **Scalable Operations:** Develop ability to operate and survive during operations conducted by large-scale threats

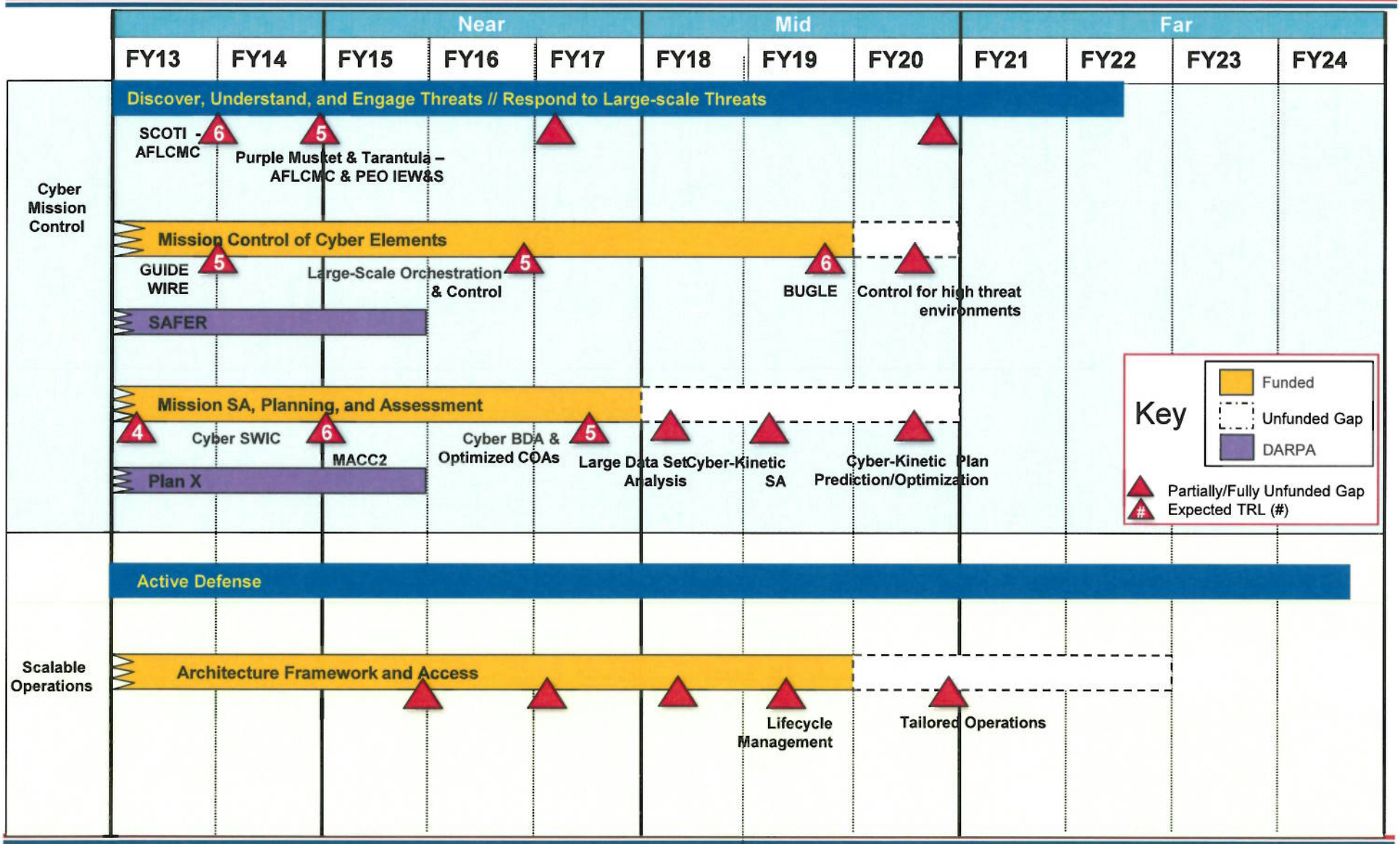
Accomplishments:

- Promised last year for FY13
  - OSD: Purple Musket
  - Navy: Flying Squirrel BT Integration
- FY13/14 AF: Mission Aware Cyber C2 (MACC2)

Technical Challenges:

- Tools for mapping and real-time analysis of missions to enable cyber/kinetic situational awareness
- Understanding dynamically evolving missions and their dependencies, identifying cyber/kinetic change indicators, updating models and resolving cross-dependencies, projecting change trends
- Decision Support and reasoning tools that factor in multiple dimensions (e.g., attribution, severity, reversibility of effect, BDA, …)

Assuring Effective Missions Roadmap

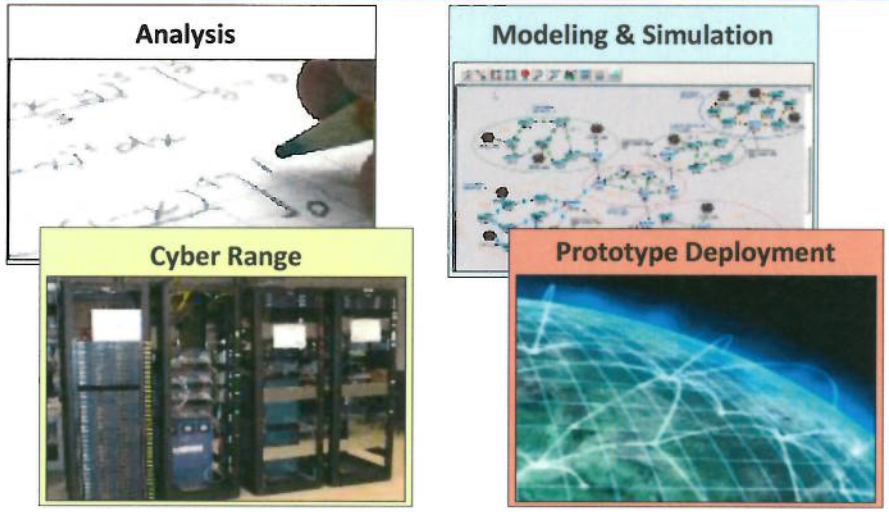


Modeling, Simulation, & Experimentation

Objectives / Accomplishments / Challenges

Objectives:

- **Simulation and Experimentation Technology**:
  - Enable robust, quantifiable, and repeatable assessment and validation of candidate cyber technology
- **Models & Analysis:**
  - Simulate the cyber operational environment with high fidelity
  - Describe and predict interactions and effect between physical and cyber domains



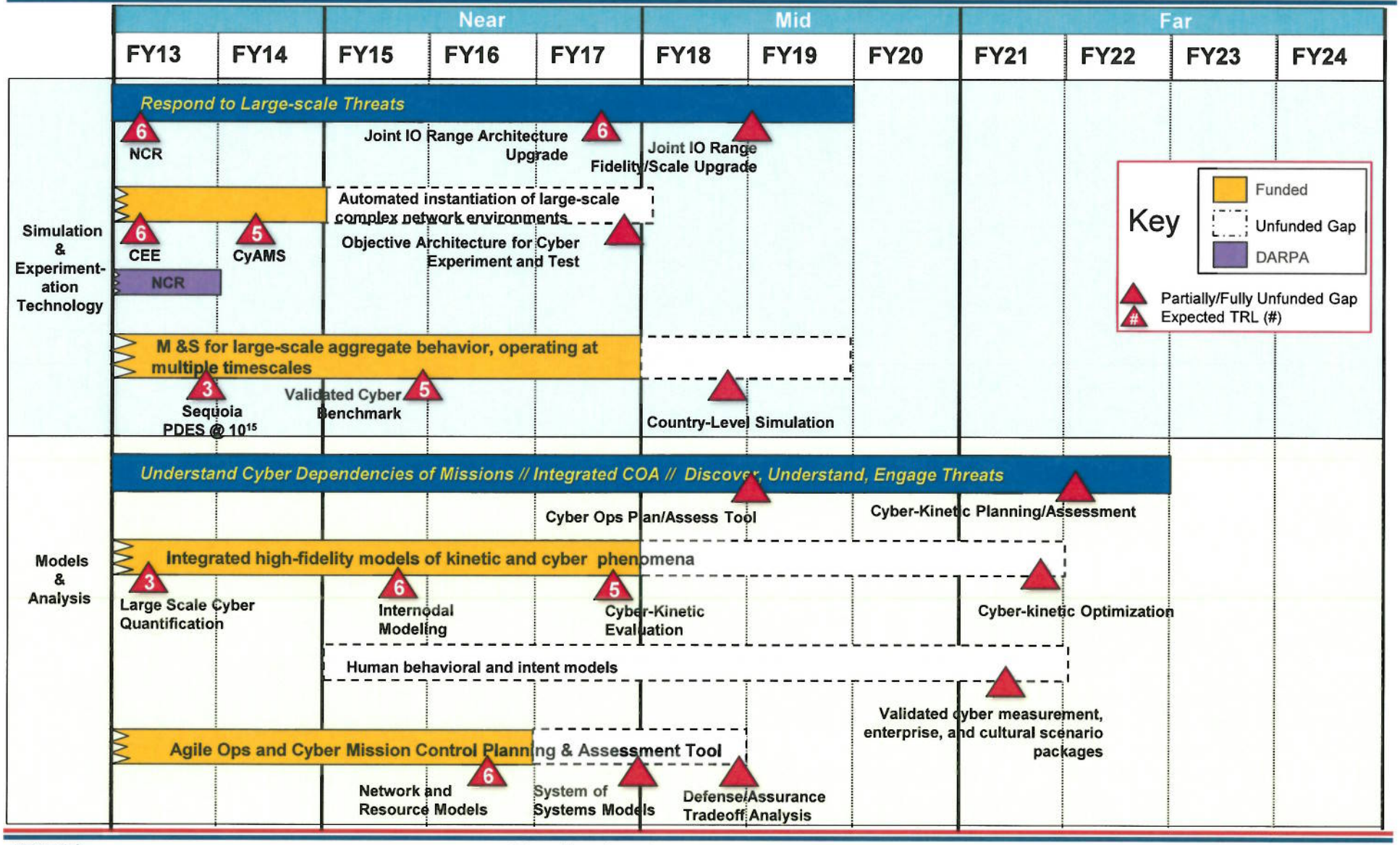
Accomplishments:

- Sequoia HPC achieved world record 10^{15} events/sec
- Army: Cyber Army Modeling & Simulation (CyAMS)
- AF: Cyber Experimentation Environment

Technical Challenges:

- Automated, rapid instantiation of large-scale, complex computing and network environments
- Objective architecture for heterogeneous range component integration and synchronization
- M&S for large-scale aggregate Internet behavior, operating at multiple timescales
- Integrated high-fidelity models of kinetic and cyber phenomena
- Human behavioral and intention models
- Planning and Assessment algorithms to evaluate operational agility and assurance

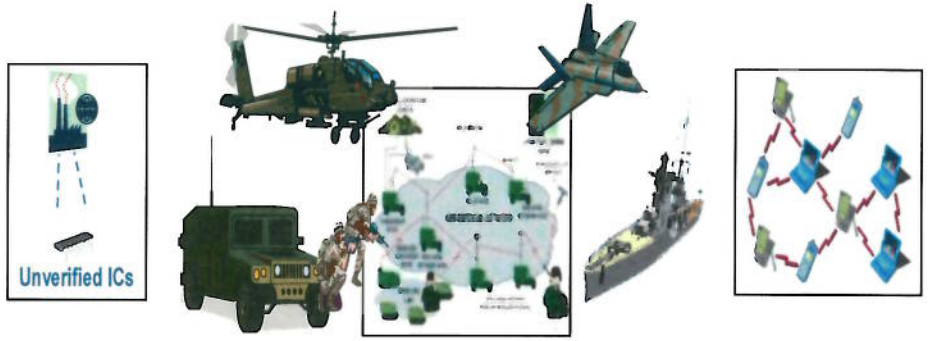
Modeling, Simulation, and Experimentation (MSE) Roadmap



Embedded, Mobile, and Tactical
Objectives / Accomplishments / Challenges

Objectives:

- **Mobile and Tactical Systems Security**
  - Secure information sharing at tactical edge
  - Reduction of mobile computing attack surface in all its aspects
- **Embedded Tactical Composite Trust**
  - Architectural approaches for composing embedded systems
  - Security capabilities needed for robust and secure composed systems
- **Leverage International Partners**



Apply the Cyber S&T Roadmap to Embedded, Mobile, and Tactical Environments

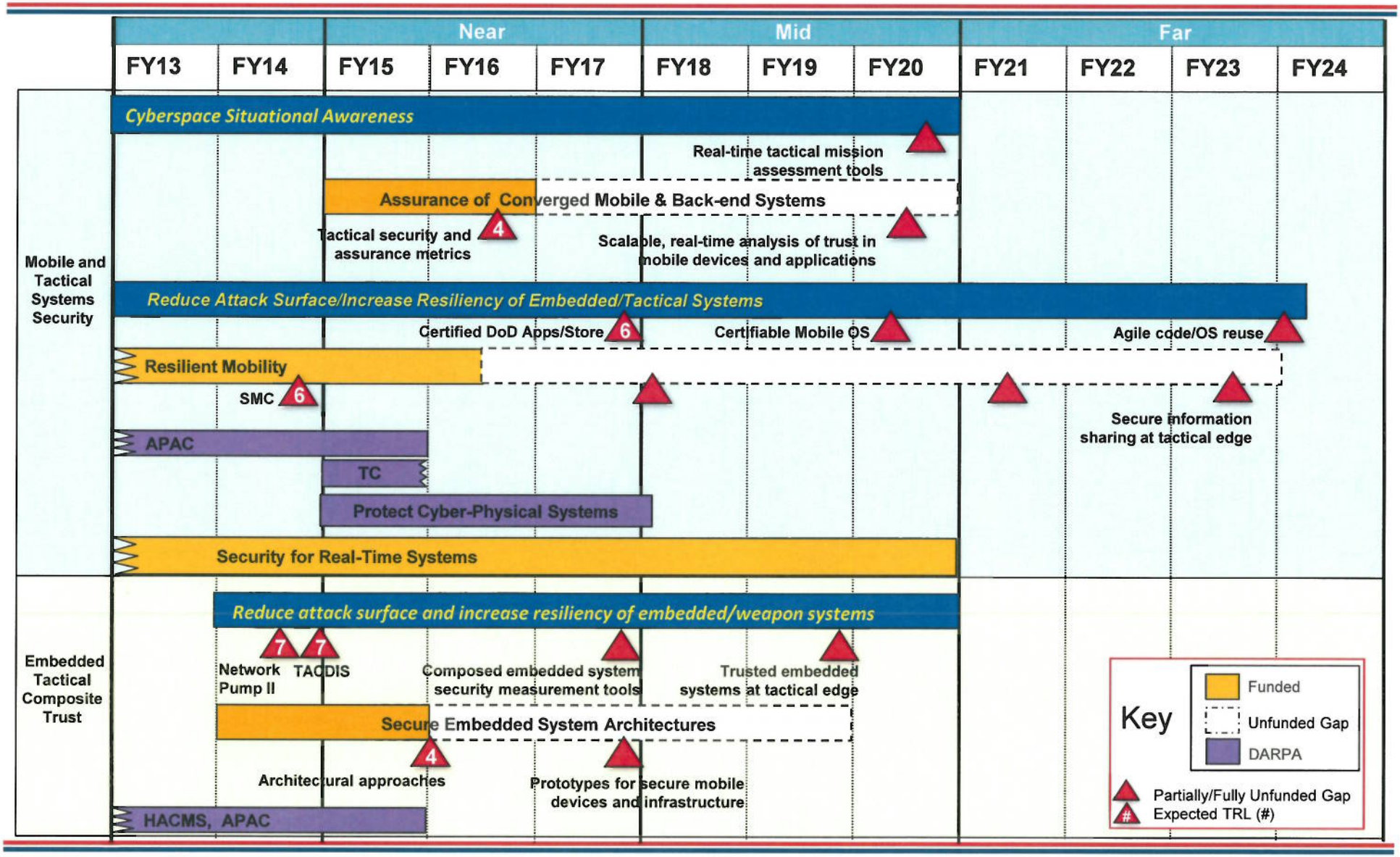
Accomplishments:

- Navy: Network Pump – II
- Army: Tactical Army Cross Domain Information Sharing (TACDIS)

Technical Challenges:

- Secure, LPI/J, energy-efficient, mobile communication protocols
- Certifiable, agile, and affordable mobile device hardware, OS, and app ecosystem
- Tools to monitor and assess assurance of cyber operations in converged strategic/tactical systems
- Self-monitoring systems in systems, including real-time integrity measurement
- Tools to monitor and assess the health and behaviors of embedded cyber systems - security of weapons systems and platforms

Embedded, Mobile and Tactical Roadmap



Outline

- BLUF
- Cyber COI Overview
- Roadmap Development Process
- Cyber COI "4 + 2" S&T Roadmaps and Recent Successes
- **Hard Problems and Gaps**
- Engagements, Way Ahead, and Opportunities
- Summary

Specific Gap Assessment

Defense

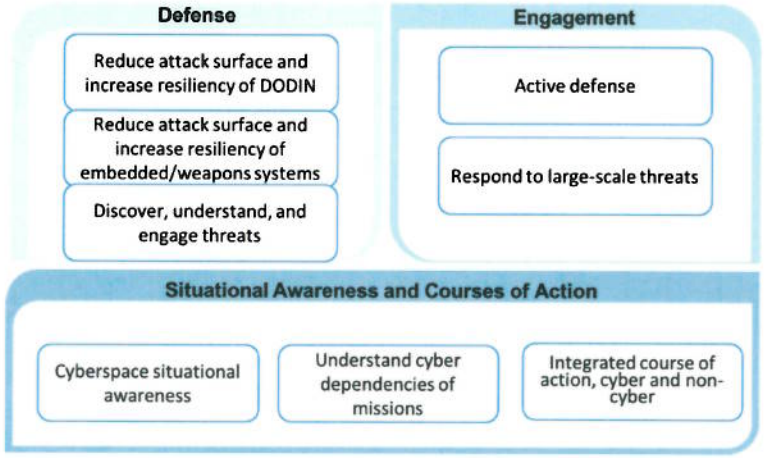
- Trustworthy embedded system architectures composed of components of mixed trust
- Trust scoring mechanisms
- Scalable HW/SW analysis and verification techniques
- Resilient mobility

Engagement

- Control planes for heterogeneous components and systems
- Threat-aware defenses
- Real-time defensive traffic management

Situational Awareness and Courses of Action

- Graded options responsive to commander's intent
- Analysis of Mission Dependencies to Cyber Infrastructure
- Cyber-Kinetic integration, planning, and assessment



Measurement and Metrics

- Quantifiable attack surface measurement
- Component and system resiliency metrics
- Threat-based agility metrics
- Calculus for Mission Assurance
- Cyber modeling and simulation and experimentation

Outline

- BLUF
- Cyber COI Overview
- Roadmap Development Process
- Cyber COI "4 + 2" S&T Roadmaps and Recent Successes
- Hard Problems and Gaps
- **Engagements, Way Ahead, and Opportunities**
- Summary

Community Engagement

- **TTCP Cyber Grand Challenge (Kickoff Jun 2014)**
  - Trust Foundations
  - Mission Assurance Through Mission Awareness (MASA)
  - Integrated Cyber-EW Operations
- **STRATCOM/J8 EW-Cyber ICD (Draft Dec 2014)**
- **Five RDA-TFs for Cyber**
- **DoD Innovation Marketplace**
  - Bi-Weekly engagement
  - AFRL IR&D Review

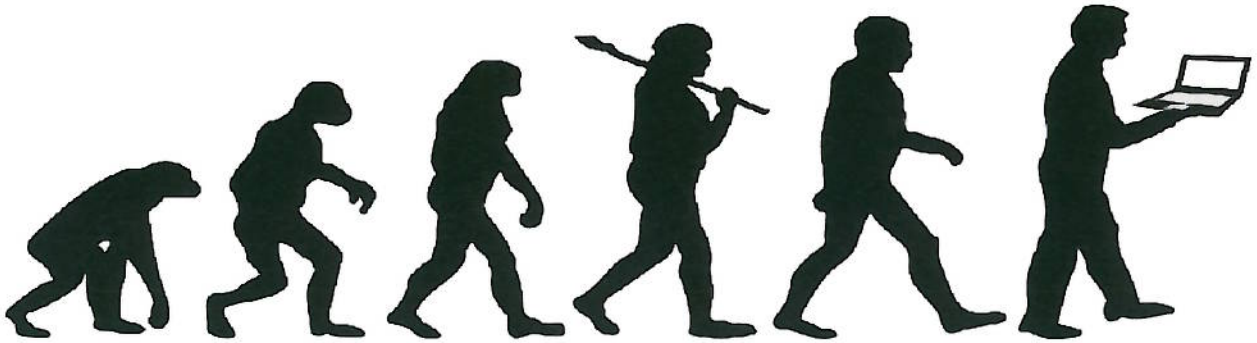
Terms:
ICD: Initial Capabilities Document
RDA-TF: Research, Development, & Acquisition Task Force
TTCP: The Technical Cooperation Panel

DoD Unique Cyber Capabilities

- **Experimentation/Assessment**
  - Cyber Experimentation Environment (CEE)
  - Army Cyber Research & Analytics Laboratory (ACAL)
  - D-Shell
  - High Performance Computing (HPC)
  - CND data sets
- **Telecommunications/Wireless**
  - Telecommunications Labs (CERDEC)
  - Communications System Integration Laboratory (CSIL)
  - HI-FI Advance Waveform and Cyber laboratory
  - Electromagnetic Environment (EME)
- **Ranges**
  - National Cyber Range (NCR)
  - Joint IO Range (JIOR)
- **Maturing Capabilities**
  - Contested Cyber Environment (CCE)
  - Network Integration Environment (NIE)

DoD Cyber Transition to Practice (CTP) Initiative

Emerging "Best of Breed" S&T Matured through Cyber Range-based T&E, Demonstrations, and Operational Pilots



- **CTP is maturing and transitioning DoD-funded cyber S&T**
  - Get S&T addressing key gaps into Ops
  - White House priority
  - Increase TRL, reduce risk
- **CTP emphasizes:**
  - Rapid results near term
  - Committed transition partner(s)
  - Co-funding by transition partner(s)
- **FY14 funding: $4.2M**
- **Two white paper rounds so far**
  - Phase 1: DoD Labs, DARPA, NSA
  - Phase 2: UARCs, FFRDCs, SPAWAR
- **8 projects underway**
- **Future**
  - Planning currently underway for next phase of CTP

Industry Engagement - Way Ahead

- **Strategic DoD-Industrial cooperation in security marketplace**
  - Metrics development
  - Standards bodies participation/voting
  - Army: Cooperative development model with industry
  - Intellectual Property business cases that reduce market friction
- **DoD-Industrial Collaboration and Co-Development**
  - Personnel Exchanges
  - Cooperative R&D Agreements (CRADA)
  - Experimentation, T&E Ranges
- **Increase speed of cyber acquisition**
  - Enhanced M&S for early assessment of S&T candidates
  - Rapid-response S&T development
    - Examples: DARPA Cyber Fast Track, AFRL ACT IDIQ…other Services also exploring similar vehicles
- **OTHER IDEAS?**

Defense Innovation Marketplace

Resources For Industry And DoD

Improve Industry understanding of DoD needs

Marketplace: Resources for DoD

- Secure portal with 10,000+ IR&D Project Summaries
- Access for DoD S&T/ R&D and Acquisition Professionals
- DoD Searchers encouraged to contact the Industry POC listed on project summaries of interest

Marketplace: Resources for Industry

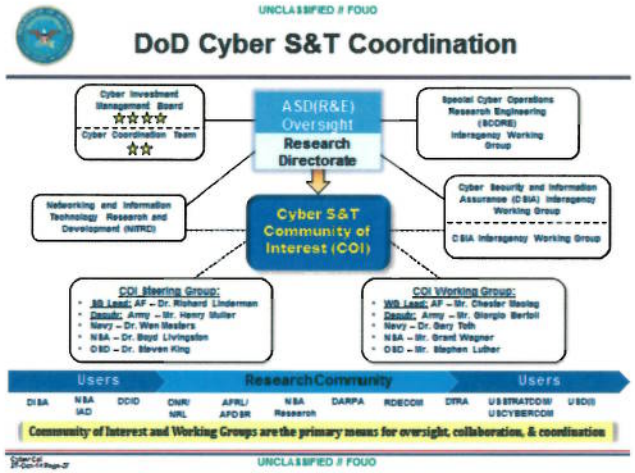
- DoD R&D Roadmaps; Investment Strategy
- Business Opportunities with the DoD
- Virtual Interchanges & Events
- Secure Portal for IR&D Project Summaries
- Top Downloads/Pages visited
- DoD IR&D SEARCH Trends

www.DefenseInnovationMarketplace.mil

Additional Resources

- **DIA Needipedia (http://www.dia.mil/Business/Needipedia.aspx)**
  - Provides a direct channel of Defense Intelligence Agency (DIA) needs into the emerging technology community
- **FedBizOps (https://www.fbo.gov/)**
  - Portal into government acquisitions providing a centralized repository for federal contract opportunities.
- **SBIR Announcements (http://www.dodsbir.net)**
  - Resource center for DoD SBIR
- **For more information on DoD cyber Science & Technology news, research needs and engagement opportunities, visit:**
  - Army Research Office (ARO)/Army Research Lab (ARL) (http://www.arl.army.mil)
  - Office of Naval Research (ONR) (http://www.onr.navy.mil)
  - Naval Research Laboratory (NRL) (http://www.nrl.navy.mil)
  - Air Force Office of Scientific Research (AFOSR) (http://www.afosr.af.mil)
  - Defense Advanced Research Projects Agency (DARPA) (http://www.darpa.mil)

Contacts



- **SG Lead: Dr Richard W. Linderman**
  - Cyber COI Steering Group Chair
  - AFRL/RI Chief Scientist
  - (315) 330-4512
  - Richard.Linderman@us.af.mil

- **WG Lead: Mr. Chester Maciag**
  - Cyber COI WG Chair
  - AFRL/RI Principal Cyber S&T Strategist
  - (315) 330-2560
  - Chester.Maciag@us.af.mil

- **OSD SG Rep: Dr Steven King**
  - OSD SG Rep
  - OASD(R&E) Deputy Director Cyber Technologies
  - (571) 372-6710
  - Steven.E.King.50.civ@mail.mil

- **Army SG Rep: Mr. Henry Muller**
  - CERDEC Acting Director
  - POC: Mr. Giorgio Bertoli
  - (443) 861-0743
  - Giorgio.Bertoli.civ@mail.mil

- **Navy SG Rep: Dr. Wen Masters**
  - Office of Naval Research
  - POC: Dr. Gary Toth
  - (703) 696-4961
  - Gary.Toth@navy.mil

- **NSA SG Rep: Dr. Boyd Livingston**
  - NSA/R Chief Scientist for Research
  - POC: Dr. Grant Wagner
  - (443) 634-4200
  - gmw@tycho.nsa.mil

Summary

- Established, mature, and coordinated community
- Cyber S&T aligned to expanding operational capability gaps/priorities
- Cyber S&T contributions to nearly all Seven DoD Hard Problems
- Driving deeper engagement with industry and international partners

BACKUP

DoD Cyber Ecosystem